Department of Homeland Security Daily Open Source Infrastructure Report for 14 March 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- Tech Web News reports the unfolding debit card scam that rocked Citibank last week, and that has now struck both national and small banks, is far from over and the first−ever mass theft of PINs is the worst consumer scam to date. (See item 13)
- The Associated Press reports passengers were taken off an Alaska Airlines plane Sunday, March 12, after a federal air marshal found a bullet in the cabin. (See item 15)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 13, Associated Press* — **Pertamina, Exxon to operate Cepu oil block.** Indonesia's Pertamina and Exxon Mobil Corp. agreed Monday, March 13, to jointly operate the country's largest untapped oil field, ending a four−year dispute that has shaken foreign investor's confidence in Indonesia. Under the agreement, Pertamina and Exxon will run the block on the border of the central and east Java provinces under a 30−year production−sharing contract with the government, according to a joint press release. Indonesia, the sole Southeast Asian member of the Organization of Petroleum Exporting Countries, or OPEC, recorded a US$7.3 billion oil trade deficit in 2005 due to faltering investment in the petroleum exploration sector.
Source: http://biz.yahoo.com/ap/060313/indonesia_oil_dispute.html?.v =1

2. *March 13, CNN* — **Gas prices up even as crude goes lower.** Prices jumped nearly 11 cents over the past two weeks to $2.35 for a gallon of regular−grade gasoline, even though the price of crude oil dropped, a national survey said Sunday, March 12. The hike obliterates the nine−cent drop that had begun January 20, said Trilby Lundberg, publisher of the Lundberg Survey. "Those five weeks of declines were due largely to our being at the bottom of our gasoline−demand curve," she said. The price rise came even as the cost of a barrel of crude fell from $62.91 on February 24 to $59.96 on Friday, March 10 −− a seven−cent−per−gallon drop. Lundberg said an expected increased demand for gasoline in the spring and new government gasoline formulation requirements combined to drive up prices at the pump. Prices are not likely to fall any time soon, she said.
Source: http://www.cnn.com/2006/US/03/12/gas.prices/index.html

3. *March 10, Lexington Herald−Leader (KY)* — **Senate passes mine safety bill lacking House's protection measures.** The Kentucky state Senate passed a mine safety bill on Friday, March 10, that lacks several miner−protection measures contained in legislation already approved by the House. Left out were requirements that would double the number of routine mine inspections per year to four, put wireless communications devices in mines, provide tracking devices for miners to help locate disaster victims, and make it illegal to alter an accident scene. House Speaker Jody Richards, D−Bowling Green, described the Senate bill as "adequate" but "concerning." He said the House would likely amend the bill to reincorporate several safety measures, then send it back to the Senate for concurrence. If the Senate refuses to yield, differences will likely be left for a committee of legislators from both chambers to hash out during the final days of the legislative session, which ends April 11. United Mine Workers of America lobbyist Steve Earle said the union won't publicly support a bill that doesn't include tracking devices and increased inspections.
Source: http://www.kentucky.com/mld/kentucky/14069146.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *March 13, WTAP News (WV)* — **Hazardous chemical leak in West Virginia prompts evacuation.** A chemical leak in Parkersburg, WV, evacuated at least a couple dozen people from their homes, a restaurant and a flea market Sunday night, March 12. The leak was hydrochloric acid coming from a stationary train tanker car, which authorities say was carrying approximately 197,000 pounds of the chemical. Residents within a 150−foot radius were evacuated.
Source: http://www.wtap.com/news/headlines/2451202.html

5. *March 12, Daytona Beach News−Journal Online (FL)* — **Carbon monoxide leak forces hotel to evacuate.** Two floors of the Plaza Ocean Club Hotel in Daytona Beach, FL, were evacuated Sunday, March 12, and six people taken to an area hospital after elevated levels of carbon monoxide were found in two guests who called 911 complaining of flu−like symptoms, a fire official said. Firefighters found the two top floors of the 11−story hotel had elevated levels of carbon monoxide. All guests were evacuated from those floors. By late afternoon, they located the leak and allowed the guests to return after determining the carbon monoxide no longer

posed a health risk to guests.
Source: http://www.msnbc.msn.com/id/11803987/from/RSS/

[Return to top]

Defense Industrial Base Sector

6. *March 11, U.S. Department of Defense* — **Ending IED threat remains top priority, President says.** Improvised Explosive Devices (IEDs) pose the biggest threat to U.S. service members and the future of a free Iraq, President Bush said Saturday, March 11, in his weekly radio address. Bush said he is dedicating "every available resource, the ingenuity of our best scientists and engineers and the determination of our military to defeat this threat." With this goal in mind, Bush said his administration has established a new high−level command at the Department of Defense, led by retired Army General Montgomery Meigs, former commander of U.S. Army forces in Europe and NATO's peacekeeping force in Bosnia. The Joint IED Defeat Organization comprises representatives from all services as well as retirees, all dedicated full−time to defeating the IED threat.
Source: http://www.defenselink.mil/news/Mar2006/20060311_4459.html

7. *March 10, GovExec* — **Military contractor ordered to pay $10 million for Iraq overcharging.** A jury has ordered Custer Battles, a military contractor, to pay $10 million for fraudulently billing the government on Iraq reconstruction contracts. The jurors in the federal courthouse in Alexandria, VA, found Thursday, March 9, that Custer Battles and its owners, Scott Custer and Michael Battles, had overcharged the government on a contract to replace old Iraqi currency with new bills. Damages were calculated at $3 million, an amount that gets tripled under federal law. Under the False Claims Act, private citizens can bring cases against companies they believe have defrauded the government, even if −− as in this situation −− the Justice Department decides not to pursue the case. The case raised the legal question of whether the False Claims Act could be applied when contractors were paid with funds that came through the currency contract and not directly from the U.S. government. In this case, the judge ruled that the False Claims Act applied because the currency contract was funded by the federal government.
Source: http://www.govexec.com/story_page.cfm?articleid=33586&dcn=to daysnews

8. *March 09, U.S. Department of Defense* — **Among European Command's needs: non−lethal capability, assured information networks, upgrades in satellite communications.** U.S. European Command's ability to transform and achieve U.S. national security objectives depends on investment in critically important areas, the command's leader said Wednesday, March 8. U.S. European Command maintains operational responsibility for Europe and most of Africa. "Your support to our infrastructure programs over the next three years is critical," Marine General James L. Jones said in a prepared statement to the House Armed Services Committee. The command's operational needs include non−lethal capabilities, and combined command, control, communications, computers and intelligence surveillance and reconnaissance, known as C4ISR. He also said it's imperative that such investments include information sharing, electromagnetic spectrum access, and assured information networks. Upgrades and continued investment in satellite communications and intelligence systems are also needed, he said.

Source: http://www.defenselink.mil/news/Mar2006/20060309_4443.html

[Return to top]

Banking and Finance Sector

9. *March 13, Federal Computer Week* — **Minnesota governor offers data privacy proposals.** Minnesota's governor wants to restrict access to the state's public records to prevent identity theft. Governor Tim Pawlenty introduced several proposals March 2 designed to improve personal data protection and stem the rising tide of identity theft. They include making driver's license data private, limiting the use of Social Security numbers as identifiers and protecting phone records. Pawlenty also wants to reform the way state agencies handle and maintain personal data. Under the current Minnesota Data Practices Act, government information is publicly accessible unless a specific law or statute designates it as private. Pawlenty has ordered the Department of Administration to conduct a review of the act and introduce a bill to reform it.
   Source: http://www.fcw.com/article92558−03−13−06−Print

10. *March 13, Times Online (UK)* — **UK's Network Rail tax credit scam wider than first feared.** Hundreds more UK rail workers have been hit by a tax credit fraud that involved stolen identities. Network Rail, the authority responsible for the UK's railway network, which became aware that many of its staff had had their identities stolen by scammers this year, believes that the final tally of victims is more than 5,300 −− a fifth higher than first thought. One in six staff at the rail group now fear that they have been caught up in a tax credit fraud that has plunged the tax system into chaos.
    Source: http://business.timesonline.co.uk/article/0,,9069−2082815,00 .html

11. *March 13, Stuff (New Zealand)* — **Identity criminals targeting New Zealand.** New Zealand is being targeted by transnational criminal groups intent on committing identity crime, says the head of the New Zealand Police's Identity Intelligence Unit. Speaking at a Biometrics Institute conference in Wellington on Friday, March 10, Neil Hallett said the use of identity crime in New Zealand to support terrorism overseas was a real threat. There is already one outstanding warrant in New Zealand for a man suspected of using identity fraud to steal hundreds of thousands of dollars to send overseas, where it will likely be used for terrorism. New Zealand passports in particular are highly sought after, he says.
    Source: http://www.stuff.co.nz/stuff/0,2106,3602387a28,00.html

12. *March 13, Bloomberg* — **Capital One to buy North Fork.** Capital One Financial Corp., the fourth−largest issuer of Visa and MasterCards, will buy North Fork Bancorp for $14.6 billion, almost doubling the company's deposits and giving it more than 50 million customer accounts. Capital One of McLean, VA, will pay $31.18 in cash and stock for each share of North Fork, the two companies said in a statement Sunday, March 12. The acquisition will increase Capital One's deposits to more than $84 billion and boost its assets to about $146 billion, ranking ahead of Cleveland−based National City Corp., the eighth largest U.S. bank as of December 31.
    Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=aVkUBC1Q9yto&refer=us

13. *March 09, Tech Web News* — **PIN scandal "worst hack ever" −− Citibank only the start.** The unfolding debit card scam that rocked Citibank last week, and that has now struck both national and small banks, is far from over, said Aviviah Litan, Gartner research vice president, Thursday, March 9, as she called this first−time−ever mass theft of PINs "the worst consumer scam to date." "It's significant because not only is it a really wide−spread breach, but it affects debit cards, which everyone thought were immune to these kinds of things," said Litan.
Source: http://techweb.com/wire/security/181502468

[Return to top]

Transportation and Border Security Sector

14. *March 13, Associated Press* — **Northwest buys FLYi operating certificate.** Northwest Airlines Corp. said it has bought the operating certificate of bankrupt FLYi Inc., a key move toward starting a new subsidiary for regional flying. Northwest will pay $2 million for the certificate, FLYi disclosed in a bankruptcy court filing. The Federal Aviation Administration requires airlines to have operating certificates, and buying someone else's is considered easier than completing the paperwork to start one from scratch. Northwest said it hopes to "accelerate the development of this subsidiary" by buying the certificate. The disclosure comes just days after Northwest reached a tentative agreement with its pilots that would allow it to form a subsidiary to fly jets with up to 76 seats. The agreement also gives Northwest's 700 laid−off pilots the first right to any jobs at the subsidiary. It also caps its size at 90 jets unless additional jets are matched one−for−one by new jets flown by mainline Northwest pilots. FLYi was the parent company of Independence Air, based in Chantilly, VA, which shut down January 5 after about a year and a half of operation. FLYi filed for Chapter 11 protection in November.
Source: http://biz.yahoo.com/ap/060310/northwest_subsidiary.html?.v= 5

15. *March 13, Associated Press* — **Bullet found on Alaska Airlines plane.** Passengers were taken off an Alaska Airlines plane Sunday, March 12, after a federal air marshal found a bullet in the cabin, the airline said. Airline spokesperson Caroline Boren said Transportation Security Administration agents found no gun or any other items of concern during a subsequent search of the San Francisco−bound aircraft. Boren said she did not know what happened Sunday, but noted that the airline flies many hunters to Alaska, and that from time to time, bullets have fallen out of passengers' pockets.
Source: http://news.yahoo.com/s/ap/20060313/ap_on_re_us/brf_bullet_on_plane;_ylt=Au.c_Dy6flqJPdmH.82LRq5G2ocA;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

16. *March 13, State (SC)* — **Ports Authority seeking to partner with private companies.** The South Carolina State Ports Authority is seeking to partner with private companies as it races to expand and match growing competition on the Atlantic and Gulf coasts. The authority wants partners for expansions planned at the former Navy base in Charleston and in Jasper County, said its new chairman, Bill Stern. Ports up and down the south Atlantic coast and into the Gulf of Mexico have announced public−private partnerships and expansions totaling billions of dollars. All involved in the ports debate agree South Carolina must continue to expand its port to satisfy customers. The State Ports Authority has been working on expansion since 1989. The

authority hopes to get the necessary permits this summer to add three berths at the former Charleston Naval Base. The cost of expansion is why the authority has soliciting private participation, Stern said. The navy base expansion is expected to cost about $600 million, and a Jasper County expansion could be upward of $1 billion.
Source: http://www.thestate.com/mld/thestate/business/14078886.htm

17. *March 13, Canadian Press* — **Toronto's Pearson Airport developing biometric security program for travelers.** The company that operates Canada's Toronto's Pearson International Airport has signed an agreement announced Monday, March 13, aimed at developing a biometric security program for travelers. The company said it will work with the Greater Toronto Airports Authority to develop a program at Pearson to allow enrolled passengers to use a dedicated security lane. Travelers who volunteer to participate would be required to complete an online application, provide biometric data −− fingerprint and iris images −− and pass an assessment. The program already operates at Orlando International Airport in Florida and has about 17,000 enrolled members.
Source: http://www.canada.com/nationalpost/news/story.html?id=3c630a5a−2d92−4c49−8858−cec4408672fe&k=33422

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

18. *March 13, Agricultural Research Service* — **Kitchen meets farm in fight against late blight.** Scientists with the Agricultural Research Service (ARS) are finding unconventional uses for such culinary classics as oregano and thyme. ARS plant pathologist Modesto Olanya and colleagues are investigating plant essential oils −− including oregano, thyme and lavender −− and other biologically based approaches to control one of the most devastating potato diseases worldwide: late blight. Potato plants infected with the fungus Phytophthora infestans may be rapidly defoliated and destroyed. The fungal disease is a formidable disease to fend off. It quickly gains resistance to widely used systemic fungicides. Olanya has found that among the essential oils, oregano is showing the greatest promise as a late blight suppressor. In laboratory tests, the researchers found that oregano and other essential oils greatly inhibited the growth of P. infestans fungi. If future studies continue to show promise, natural remedies such as essential oils could someday reduce a portion of the many fungicides used to prevent late blight from taking root in U.S. potato fields each year. To increase their efficacy, Olanya is looking at pairing essential oils with other natural products, such as beneficial microorganisms.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

19. *March 13, Hutchinson News (KS)* — **Farms and ranches still vulnerable.** The Kansas Bureau of Investigation received a $233,832 federal grant in 2003. The grant supported a research project on terrorism and agriculture. The report found: law enforcement strategy toward the

threat posed by agricultural terrorism remains largely reactive, if not passive; with the exception of a few county sheriffs, law enforcement agencies have not developed strategies to protect agriculture, nor have they developed coordinated emergency response plans to deal with foreign animal disease outbreaks; law enforcement intelligence concerning threats to agriculture is virtually nonexistent. State and federal intelligence networks receive little, if any, criminal information from local law enforcement concerning suspects and suspicious activities related to the agriculture industry.
Source: http://www.hutchnews.com/news/regional/stories/farms031306.h tml

20. *March 12, Xinhua (China)* — **Foot−and−mouth outbreak confirmed in Qinghai.** An outbreak of Asia Type One foot−and−mouth disease has occurred in a village called Dayu in Guinan County in northwestern Qinghai Province, China's Ministry of Agriculture announced on Sunday, March 12. Nineteen cattle and two pigs on the farm which reported the outbreak have been culled by the provincial veterinary bureau. The Qinghai provincial government and the Ministry of Agriculture ordered an immediate disinfection and quarantine of the outbreak site, as well as a thorough inoculation of all vulnerable animals in the region.
Source: http://news.xinhuanet.com/english/2006−03/12/content_4295359 .htm

[Return to top]

Food Sector

21. *March 13, MarketWatch* — **Hong Kong halts beef imports from U.S. company.** Hong Kong health authorities have slapped a suspension on all imports from a Colorado−based beef processor after discovering the firm had shipped meat products to the territory containing skeletal bones. Imports from the Swift Beef Company were suspended with "immediate effect," according to the airport office of the Food and Environmental Hygiene Department, citing a spot inspection of product from the company carried out Friday, March 10. Hong Kong permits only boneless beef from cattle less than 30 months old, with the animal's brain, spinal cord and other parts with a high risk of mad cow disease removed.
Source: http://www.marketwatch.com/News/Story/Story.aspx?guid=%7BC5E 432E0%2D453E%2D472A%2DB67B%2DC027FBFBB4BC%7D&dist=newsfinder &siteid=google&keyword=

22. *March 13, Xinhua (China)* — **Seoul to reconsider imports of U.S. beef if mad cow case confirmed.** South Korea may again ban imports of U.S. beef if tests confirm a suspected mad cow case in the U.S. reported Saturday, March 11, a South Korean government official said Monday, March 13. "We are keeping close tabs on the latest mad cow report and will take appropriate actions depending on the results of a more detailed test," said Lee Yang−ho, spokesperson for the South Korean Ministry of Agriculture and Forestry. Lee said that if the second test comes out positive, South Korea and the U.S. will have to renegotiate everything concerning to an earlier agreement reached between the two sides on reopening the local market to U.S. beef in early 2006. Seoul halted U.S. beef imports in late 2003 because of a confirmed mad cow case in the U.S.
Source: http://news.xinhuanet.com/english/2006−03/13/content_4297736 .htm

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

23. *March 13, Agence France−Presse* — **Myanmar battles first bird flu outbreak.** Myanmar quarantined at least four farms and began culling poultry after announcing its first outbreak of bird flu, amid fears about whether its creaking health system could deal with any human cases. The military−ruled country's top veterinary official Than Hla said no humans had been infected so far but added that "many" farms may have birds carrying the deadly H5N1 strain. Myanmar's secretive rulers informed the Food and Agriculture Organization Monday, March 13, that it had detected the H5N1 virus, which can be deadly to humans, after 112 birds died mysteriously on March 8 near Mandalay. However, Myanmar apparently made no public announcement to its people about the outbreak. Only a handful of residents in Mandalay, contacted by telephone, had heard the news on shortwave radio stations broadcasting from overseas. Myanmar, which has been ruled by the military since 1962, is one of the world's most isolated nations, but the World Health Organization said the junta was cooperating well with international organizations on bird flu.
Source: http://news.yahoo.com/s/afp/20060313/hl_afp/healthflumyanmar_060313123345;_ylt=AiDXgeKe8lmM1IP6RvGbYpuJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

24. *March 13, ABC News* — **Officials advise stocking up on provisions.** In a speech over the weekend of March 11, Secretary of Health and Human Services Michael Leavitt recommended that Americans start storing canned tuna and powdered milk under their beds as the prospect of a deadly bird flu outbreak approaches the U.S. "There's no way you can protect the U.S. by building a big cage around it and preventing wild birds from flying in and out," Secretary of Agriculture Michael Johanns said. U.S. spy satellites are tracking the infected flocks, which started in Asia and are now heading north to Siberia and Alaska, where they will soon mingle with flocks from the North American flyways. The bird flu virus, to date, is still not easily transmitted to humans. There have been lots of dead birds on three continents, but so far fewer than 100 reported human deaths. But should that change, the spread could be rapid.
Source: http://abcnews.go.com/GMA/print?id=1716820

25. *March 10, Associated Press* — **Health officials would have new power in flu pandemic.** Health officials would be given additional powers to react to a pandemic flu, including the authority to train civilians to deliver immunizations and other medical care, New York Health Commissioner Antonia Novello said Friday, March 10. Under forthcoming legislation, the health commissioner and local health officials would be able to authorize unlicensed people to deliver immunizations and other medical care. The legislation was outlined by Novello at a public hearing hosted by the state Senate on the state's flu plan. Additional legislation would authorize the health commissioner to redeploy medical equipment, and require electronic reporting of disease, and the submission clinical specimens to the state Health Department.

Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−flu plan0310mar10,0,2220400.story?coll=ny−region−apnewyork

[Return to top]

Government Sector

26. *March 10, Federal Computer Week* — **Storm−affected Louisiana residents can turn to Web portal.** Several national and local government and nonprofit organizations unveiled a new one−stop Web portal last week to help Louisiana residents displaced by Hurricanes Katrina and Rita last year get jobs, find affordable housing and receive social services. The site, called LouisianaRebuilds.info, will provide updated national and local content about resources and information related to rebuilding and planning, according to a press release.
Web portal: http://www.louisianarebuilds.info/
Source: http://www.fcw.com/article92574−03−10−06−Web

[Return to top]

Emergency Services Sector

27. *March 12, Ocala Star−Banner (FL)* — **Florida emergency agencies hone skills with chemical disaster drill.** In a disaster drill scenario in Belleview, FL, Saturday, March 11, a mock chemical explosion rocked the Belleview High School stadium, where the victims had gathered for the Special Olympics opening ceremony. This drill drew together emergency personnel from Marion, Sumter, Lake, Levy, Hernando and Citrus counties. One of the primary purposes of the drill, Marion County Fire−Rescue spokesperson Heather Danenhower said, was to test the decontamination and triage processes. While agencies won't receive an official report for several weeks, Marion County Fire−Rescue Chief Stuart McElhaney said he's confident if a similar situation actually happened here, his agency would be ready. What was evident were issues with the communication system −− something county commissioners have already committed to upgrading, McElhaney said −− and a need for more hazardous−material team members, of which there are currently 30.
Source: http://www.ocala.com/apps/pbcs.dll/article?AID=/20060312/NEW S/203120386/1001/NEWS01

28. *March 12, Lufkin Daily News (TX)* — **Texas city reviews emergency response actions.** An Emergency Management After Action Review in Lufkin City, TX, completed last month by Assistant City Manager Kenneth Williams, evaluated the city's performance during Hurricane Rita on five counts: Emergency Operations Center (EOC), shelter operations, field operations, communications and data management, and intergovernmental cooperation. Some of the review's findings include: a) Even though the functionality of the emergency operations center, located in City Hall, was described as "outstanding" in the review, it found that the center was "not controlled appropriately"; b) the review stated that "there should be a long−term shelter solution with expansion of the hub system. Cities north and west such as Tyler, Longview, Bryan, Dallas and Fort Worth should be included in the hub plan"; c) vital information was needed to be communicated to departments such as public works, information technology,

police department/command and dispatch, and the state regional liaison officer; d) the city established a phone bank system, for the first time, in conjunction with the EOC. Though this worked well, the review stated, communicating messages between the EOC and the phone bank to the appropriate person or agency must be improved.
Source: http://www.lufkindailynews.com/news/content/news/stories/2006/03/12/20060312LDNrita.html

29. *March 12, New Jersey Herald* — **New Jersey first responders attend conference.** New Jersey police, firemen, public health officers and other emergency responders experienced a terrorist threat firsthand Friday, March 10. The staged event, which included a showdown between a soldier and a suicide bomber, was part of a two−day conference held at New Jersey's Picatinny Arsenal to prepare emergency workers for a variety of situations they could encounter. About 290 people from around the state attended the conference, sponsored by Picatinny, the University of Medicine & Dentistry of New Jersey, the Morris and Warren county health departments, the state Department of Health and Senior Services and the state Society for Public Health Education. A panel of army researchers from around the country provided participants with the latest information on topics including chemical protection, simulators and communication.
Source: http://www.njherald.com/339410945121105.php

30. *March 11, South Bend Tribune (IN)* — **Response policies lacking in Indiana county, new emergency management agency director says.** In a board meeting Thursday, March 9, Clyde Avery, newly appointed Marshall County, IN, Emergency Management director, detailed the lack of documented policies for emergency response, all of which will be required by the federal National Incident Management System. Additionally, many agencies that will be called upon during a disaster, whether natural or man−made, have too many tasks to perform than "is realistically possible," Avery told the group. Additionally, Dr. Byron Holm, Plymouth physician, cited the 12−minute time frame it took to notify all the required emergency agencies about last week's tornado warning drill, saying future grant money should be directed to improving communications.
Source: http://www.southbendtribune.com/apps/pbcs.dll/article?AID=/20060311/News01/603110330/−1/NEWS01/CAT=News01

31. *March 10, Congress Daily* — **Military says training, gear needed for future disasters.** The National Guard is beginning to address flaws in its response to Hurricane Katrina, but more work and money is needed to better prepare the state−run units to respond to catastrophes, the chief of the National Guard Bureau said Friday, March 10. The Guard particularly needs a boost in funding for new gear. To make up for the shortfalls, states have signed equipment−sharing compacts. But Lt. General Steven Blum said he feared those agreements may not be enough to prepare the Guard to respond quickly to domestic disasters. Blum said the dearth of equipment would hamper his force's ability to respond to multiple events in several states at once.
Source: http://www.govexec.com/story_page.cfm?articleid=33590&dcn=to daysnews

[Return to top]

Information Technology and Telecommunications Sector

32. *March 13, Federal Computer Week* — **Mobile computing and larger databases pose new risks for unprotected data.** As more companies disclose information losses and data theft, information technology companies have entered the market to sell products that encrypt entire hard drives. Those companies argue that encrypting all data on a disk is the best way to protect it from internal and external threats, including user carelessness. “It means the user can never make a mistake” that jeopardizes data security, such as putting classified material in an unclassified folder or onto a portable storage device, said Matt Pauker, co−founder of Voltage Security.
Source: http://www.fcw.com/article92554−03−13−06−Print

33. *March 13, Register (UK)* — **Virtual rootkits create stealth risk.** Security researchers have uncovered new techniques to hide the presence of malware on infected systems. By hiding rootkit software in virtual machine environments, hackers have the potential to avoid detection by security software, experts at Microsoft Research and the University of Michigan warn. Existing anti−rootkit tools commonly rely on comparing file system and API discrepancies to check for the presence of rootkits, a technique that wouldn't be able to unearth virtual machine malware.
Source: http://www.theregister.co.uk/2006/03/13/virtual_rootkit/

34. *March 11, Security Focus* — **Apple QuickTime/iTunes integer and heap overflow vulnerabilities.** An integer overflow and heap−based buffer overflow vulnerability have been reported in Apple QuickTime and iTunes. These issues affect both Mac OS X and Microsoft Windows releases of the software. Analysis: A successful exploit will result in execution of arbitrary code in the context of the currently logged in user. Vulnerable: Apple QuickTime Player 7.0.4; Apple QuickTime Player 7.0.3; Apple iTunes 6.0.2; Apple iTunes 6.0.1. Solution: Security Focus is currently not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/17074

35. *March 11, Associated Press* — **Students learn about cybersecurity via pilot program.** A group of students at Rome Catholic School in Rome, NY, are learning how to become the future defenders of cyberspace through a pilot program that officials say is the first of its kind in the country. The program teaches students about data protection, computer network protocols and vulnerabilities, security, firewalls and forensics, data hiding, and infrastructure and wireless security. Most importantly, officials said, teachers discuss ethical and legal considerations in cyber security. The pilot program was developed with help from computer experts at the U.S. Air Force's Research Lab in Rome, who four years ago created a 10−week Advanced Course in Engineering Cyber Security Boot Camp for the military's Reserve Officers Training Corps, said Kamal Jabbour, the lab's principal computer engineer. The material covered in the course is subject matter that college students typically don't receive until their junior year.
Source: http://www.wired.com/news/wireservice/0,70396−0.html?tw=rss. index

36. *March 10, Tech Web* — **Free search engine identifies unknown Windows files.** Bit9 Inc. on Monday, March 13, launched a free search engine to identify unfamiliar software applications and executables found on any computer running the Windows operating system. Users will be able to download a utility at Bit9's Website to tap into the firm's 4−terabyte database. The database holds approximately 25 million unique files and 250 million records to source and

identify the software. Bit9 expects to triple the data by the end of the year.
Bit9's database: http://fileadvisor.bit9.com/services/search.aspx
Source: http://www.techweb.com/wire/security/181502659;jsessionid=FX UUHIAQQXJHEQSNDBECKHSCJUMEKJVN

37. *March 09, IDG News Service* — **Microsoft to issue critical patch Tuesday.** In its monthly patch release Tuesday, March 14, Microsoft will issue one critical security bulletin concerning the Office suite and one bulletin on Windows that is rated important, the company said Thursday, March 9. Also Tuesday, Microsoft will release an updated version of the Microsoft Windows Malicious Software Removal Tool, according to an advisory.
More information on the updates can be found at:
http://www.microsoft.com/technet/security/bulletin/advance.m spx
Source: http://www.infoworld.com/article/06/03/09/76296_HNmscritical oatch_1.html?source=rss&url=http://www.infoworld.com/article /06/03/09/76296_HNmscriticaloatch_1.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for a vulnerability in Apple Safari Browser. The Apple Safari browser will automatically open "safe" file types, such as pictures, movies, and archive files. A system may be compromised if a user accesses an HTML document that references a specially crafted archive file. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary commands with the privileges of the user.

More information can be found in the following US−CERT Vulnerability Note:

VU#999708 − Apple Safari may automatically execute arbitrary shell commands
http://www.kb.cert.org/vuls/id/999708

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:

Disable the option "Open 'safe' files after downloading," as specified in the Securing Your Web Browser
http://www.us−cert.gov/reading_room/securing_browser/#sg eneral

Current Port Attacks

Top 10 Target	1026 (win−rpc), 6711 (BackDoorG), 445 (microsoft−ds), 25 (smtp), 12106 (−−−), 6658 (−−−), 139 (netbios−ssn), 113 (auth), 80 (www),

Ports	32774 (sometimes−rpc11) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.